Future Challenges Risk

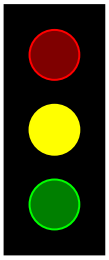
We are working to promote a culture that rewards unconventional thinking – a climate where people have freedom and flexibility to take risks and try new things…one that does not wait for threats to emerge and be "validated," but rather anticipates them before they emerge – and develops and deploys new capabilities quickly, to dissuade and deter those threats.

Secretary of Defense Donald H. Rumsfeld
February 5, 2003

The most reliable barometer of transformation in the defense community is to observe how the culture is changing. How and why are things done differently than in the past? How are those changes redefining what we believe we need to accomplish next? For that reason, the Department's progress toward transformation is best measured by observing the number and character of activities that lead the defense community to fundamentally new relationships, and thus to "transformed" capabilities.

The Secretary's performance priorities for future challenges risk in FY 2005 are *Transform the Joint Force* and *Optimize Intelligence Capabilities.*

DRIVE INNOVATIVE JOINT OPERATIONS



Fashioning joint operating concepts to guide the conduct of joint operations is our leading priority for transformation. We continue to support the six transformational goals identified in our 2001 defense review:

- Defend the U.S. homeland and bases of operation overseas;
- Project and sustain forces in distant theaters;

- Deny enemies sanctuary;
- Improve our space capabilities and maintain unhindered access to space;
- Harness our advantages in information technology to link up different kinds of U.S. forces, so they can fight jointly; and
- Protect U.S. information networks from attack -- and to disable the information networks of our adversaries.

During FY 2005, we plan to spend approximately $30 billion on transforming military capabilities that will support each of these critical objectives.

Maintained Balanced and Focused Science and Technology

We intend to increase spending for research and development by 50 percent above the 2002 baseline budget by FY 2008. During FY 2005, we proposed spending $68.9 billion on research and development, an increase of about 45 percent from the FY 2002 President's Budget baseline of $47.4 billion. Within the total research and development account, science and technology funds are those defense dollars spent on basic research, applied research, and advanced technology development. To make sure key priorities are supported by these funds, the Director of Defense Research and Engineering has set individual targets for each component of the Department's overall science and technology program:

- ***Basic Research: 15 percent***. Often called the "seed corn" of military technology, basic research is the systematic study of fundamental aspects of science without any specific application, such as a weapon system, in mind.
- ***Applied Research: 35 percent***. Applied research translates promising basic research into solutions for broadly defined military needs by exploring ways to design, develop, or improve prototype devices, materials, or systems.
- ***Advanced Technology Development: 50 percent***. Advanced technology is the last steps in the process, demonstrating how a new idea can increase military capabilities or reduce costs

when applied to different types of military equipment or techniques.

Experiment With New Warfare Concepts

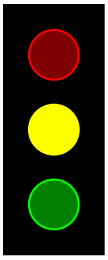
The Commander of the Joint Forces Command in Norfolk, VA is responsible for driving major change in how we think about fighting and winning on the battlefield, in harmony with the joint concepts identified in the Secretary's annual update to the Transformation Planning Guidance. He oversees more than 800 military and government workers, contractors and consultants who constitute a massive "transformation laboratory."

During FY 2003, the Joint Forces Command hosted three major wargames (Unified Quest, Unified Course, and Pinnacle Impact 03) and many other smaller experiments to test new concepts of joint command and control. During FY 2004, events like Unified Quest 04, a "discovery" experiment focused on applying new joint operations concepts to major combat operations, stability operations, transition to post-conflict, and the network battle-centric command in the year 2015, will build on emerging lessons learned from these earlier events.

Although this experimentation program is highly decentralized— relying on many smaller-scale experiments conducted by all players in the military and interagency community— Joint Forces Command tracks the expected manpower and funding to be invested each year, and lists the deliverables (exercises event, concept document); the command then issues periodic after-action and prototype development reports. For more discussion of ongoing and planned joint experiments and concept development, visit the Joint Forces Command website at www.jfcom.mil.

Over the past year, the experimentation program overseen by the Commander, U.S. Joint Forces Command has been aligned with the emerging joint operations concepts. Accordingly, this measure has been combined with "Joint Force Experimentation," since both activities conform to the same guidance and share management oversight.

DEVELOP MORE EFFECTIVE ORGANIZATIONS



As our culture changes, our focus shifts to enabling what we call joint operations—the ability of our land, sea, air, and space forces to be combined under the control of a single combatant commander and used in ways that are most appropriate to achieving the objectives of the campaign that he has laid out.

Strengthen Joint Operations

It is not enough to say we want to *fight* joint—we have to *think* joint, too. Accordingly, we are dedicating a substantial amount of funding to bring a joint perspective to how we structure, train, deploy, and manage forces and organizations.

TRANSFORM JOINT TRAINING

To win militarily in the new global operational environment, our forces must be trained effectively to decisively overcome asymmetric adversaries and deal with surprise. The training system of the 1990's was designed assuming a well-defined and stable opponent. However, the challenges of today demand we replace this requirements-driven training system with one that is dynamic, collaborative, and capabilities-based.

Our training transformation initiative takes a top-down approach, inviting stakeholders (combatant commanders) to participate in setting goals and defining success. The Training Transformation implementation plan (www.t2net.org), which was signed by Deputy Secretary of Defense Paul Wolfowitz on June 10, 2003, is a road map to developing and fielding dynamic, capabilities-based training for military, federal, and international partners worldwide. Much of this training will be "virtual," leveraging the most modern modeling and simulation tools.

By FY 2007, our goal is to ensure that all forces arriving for combatant command duty have been joint-trained in an innovative atmosphere that promotes the creation of new joint operational capabilities, and provides direct experience with dynamic mission planning and rehearsal tools. During FY 2004, we will develop

overarching performance architecture via a mini-symposium hosted by the Military Operations Research Society. During FY 2005 , based on this new architecture, we will introduce new courseware and content to the training syllabi used by the joint community. We also will refine the performance standards of joint training events to meet the emerging needs of the combatant commanders..

ESTABLISH A STANDING JOINT FORCE HEADQUARTERS (SJFHQ)

Three years ago we took steps to create permanent joint headquarters for each of our combatant commanders worldwide. These headquarters are being equipped with the most capable command, control, computers, communications, intelligence and surveillance asses we have available. During FY 2003, we published Joint Chiefs of Staff Instruction 3170.01C (available at www.dtic.mil) to establish performance standards and management criteria for these new organizations. Fifty-eight billets were identified that could be shifted from other assets to fill out the core of the new staff. This year, we are training regional command staffs and will conduct three exercises to test proposed operating procedures and tactics. We have already stood up a prototype SJFHQ at the Joint Forces Command, and approved SJFHQ billets for the Pacific, Central, Southern, and European Commands. The goal is to have an operational SJFHQ at all regional combatant commands by the end of 2005.

ESTABLISH A GLOBAL JOINT PRESENCE POLICY

This initiative is among several similar developmental efforts that are being combined during FY 2005 into a single, integrated protocol for global joint force management.

Enhance Homeland Defense and Consequence Management

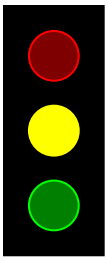
The Department has the lead in providing for the defense of the United States and is an important government partner in providing for homeland security. Defense responsibilities range from overseas military missions to planning for homeland defense under the auspices of the U.S. Northern Command, a new combatant command, and the U.S. Pacific Command. At the direction of the President or the Secretary of Defense, the Department will

undertake military missions at home to defend the United States, its population, and its infrastructure from external attack.

We are also engaged in important activities to ensure the continuity of government in case of an attack or other crisis, and provide quick-response, vital support to civil authorities in an emergency, when required by circumstances or when the need surpasses the capacities of civilian responders. Such assistance to civilian agencies could include consequence management in the event of an attack involving the use of weapons of mass destruction.

In 2004, we will complete the first comprehensive, defense-wide strategy for the Department's contribution to the national homeland defense. This new strategy will rely on an integrated threat assessment to support definition of strategic goals for the Department's role in homeland security and defense. Then during FY 2005 – and taking risk into consideration – we will describe the associated resource and technology roadmap to achieve those goals in the next defense budget. By providing an overarching suite of strategic goals aligned with resource and technology plans, we will add coherence and direction to the disparate activities across the Department now charged with deterring and preventing attacks, protecting critical defense and designated civilian infrastructure, providing situational understanding, and preparing for and responding to incidents.

DEFINE AND DEVELOP TRANSFORMATIONAL CAPABILITIES



When this Administration took office three years ago, the President charged us with a mission – to challenge the status quo, and prepare the Department of Defense to meet the new threats our nation will face as the 21st century unfolds . . . We have done a good deal to meet that charge.

Secretary of Defense Donald H. Rumsfeld
February 4, 2004

We have fashioned a new defense strategy, a new force sizing construct, and a new approach to balancing risks – one that takes into account not just the risks in immediate war plans, but also the risks to people and transformation. We have moved from a "threat-based" to a "capabilities-based" approach to defense planning, focusing not only on who might threaten us, or where, or when – but more on *how* we might be threatened, and what portfolio of capabilities we will need to deter and defend against those new threats.

Monitor the Status of Defense Technology Objectives

Our science and technology investments are focused and guided through a series of Defense Technology Objectives (DTOs), which highlight specific technological milestones to be reached. Every two years, independent peer review panels assess the DTOs – at least two-thirds of the panel members are from academia, private industry, and other U.S. government agencies. The reviews are conducted openly; observation by stakeholders is welcomed. The teams assess progress against three factors—technical approach, funding, and technical progress—and rate the programs as:

Green	Progressing satisfactorily toward goals
Yellow	Generally progressing satisfactorily, but some aspects of the program are proceeding more slowly than expected
Red	Doubtful that any of the goals will be attained.

The benefits of these ratings are many. Not only do they reflect the opinions of independent experts, but they are also accepted and endorsed by stakeholders. These reviews result in near real-time

adjustments being made to program plans and budgets based on the ratings awarded. To measure performance in this area, our overall goal is to have 70 percent or more of the DTOs progressing satisfactorily ("green" or "yellow"). The Department has exceeded this goal each year since FY 2000; however, setting a higher target may discourage research in higher risk (but also higher payoff) areas. Therefore, our performance target for FY 2004 and FY 2005 will remain at 70 percent.

In FY 2003, 96 percent of the DTOs reviewed were determined to be progressing satisfactorily. The same success rate is expected in FY 2004 and FY 2005. As the Defense Advanced Research Projects Agency (DARPA) includes a greater portion of their total science and technology investment in DTOs, the Department's aggregate success rate may drop slightly, given the high-risk nature of DARPA programs.

Exploit the U.S. Information Advantage

Our preeminent global intelligence capability is the foundation of U.S. military power. It enables our leaders to decide how and when to apply military force, and provides a capability to assure allies and friends of our purpose and resolve, dissuade adversaries from threatening ambitions, deter aggression and coercion, and decisively defeat an adversary on our terms.

ACHIEVE PREDICTIVE INTELLIGENCE CAPABILITIES AND RESPONSIVE, INTEGRATED INTELLIGENCE SYSTEMS

We are committed to developing capabilities that provide insights into our adversaries' intentions and secrets without *their* knowing that *we* know. This means closing the gap in time and culture between intelligence and military operations. To do so is to enable a seamless transition from the collection of information to its employment to assessments of the effects of that employment.

A critical step on this path is shifting from a collection-focused intelligence system to a user-driven system. This will fundamentally change the way in which we plan and operate. It will facilitate joint and combined intelligence operations and will exploit the

advantages of information technology to provide knowledge to our customers when they need it. To that end, we are researching capabilities that let users pull relevant data from any place on the intelligence network to where it is needed most, regardless of origin or format. These capabilities will not replace current intelligence, data analysis, or analysts; rather, they will capitalize on already collected information.

MAKE INFORMATION AVAILABLE ON A NETWORK THAT PEOPLE DEPEND ON AND TRUST

Moving information quickly and accurately is a vital combat multiplier. Networks have demonstrated a remarkable ability to leverage information to improve the lethality and responsiveness of combat power.

For example, during the early stages of Operation Iraqi Freedom, a forward operating base of the 2nd Brigade of the 4th Infantry Division was receiving incoming mortar fire. The radar of an artillery command and control (C2) system was able to pinpoint the source. An unmanned aerial vehicle, which was already flying in the area, verified the radar contact. The location of the enemy position was transmitted to the Advanced Field Artillery Tactical Data System (AFATDS), a totally integrated fire support C2 system that processes fire mission and other related information to coordinate and optimize the use of all fire support assets, including mortars, field artillery, cannon, missile, attack helicopters, air support, and naval gunfire. With the mortar position locked in AFATDS, the forward base could quickly launch a counter-fire mission. During initial operations for Operation Iraqi Freedom, 90 percent of our fire missions were digitally targeted, reducing the time to execute from the hours needed during Desert Storm, to just minutes.

Another important capability is to be able to "see" the battlefield, especially how friendly forces are positioned relative to a potential or active threat. The Army has had excellent success with the Blue Force Tracker (BFT), a new digital tracking system that shares information among hundreds of other commanders. The system tracks both friendly (blue) and enemy (red) forces, and allows troops

to communicate by e-mail, a good back-up if tactical radios fail or a unit moves out of transmission range.

The BFT was deployed to the 101st Airborne Division (Air Assault) and 82nd Airborne Divisions, and quickly proved its value by helping a whole squadron column moving along a highway avoid a night ambush. Using the BFT graphical representation of the battlefield, the squadron commander knew the location of all blue forces. This enabled him to quickly spot red (enemy) forces that had moved into the area and call for fire to defeat them before they could launch an attack.

Ongoing research efforts are trying to find ways to "squeeze" information so it flows more easily, consistent with lessons learned from the battlefield. As more of these new concepts and programs are fielded, we will mature our understanding of the exact relationships between technology, operations, employment protocols, and battlefield performance.

POPULATE THE NETWORK WITH NEW, DYNAMIC SOURCES OF INFORMATION TO DEFEAT THE ENEMY

Our military commanders use information of all kinds, not only intelligence data, to "see" the battle space, and thus outwit and overcome our adversaries. The net-centric enterprise architecture we are building will allow commanders to engage the network at any time from anywhere using a military version of the Internet search engine, without needing cumbersome base support. Data will be posted and ready for download and analysis as soon as it arrives, anywhere on the network.

An essential capability provided by such dynamic information is the ability to tell friend from foe on the battlefield. The dynamic information provided by the common operational picture (COP) was able to avert a potential fratricide on 1 April 2003, east of Karbala, Iraq. On that day, during a passage of lines, U.S. forces did not know that a U.S. scout platoon was in front of a tank platoon until alerted by the BFT. Without the real-time warning, the tank platoon might have targeted the scout as an infiltrating enemy force.

Dynamic information can also increase the speed and focus of combat planning and mission execution. For example, during deployment of an aircraft carrier in support of Operation Enduring Freedom after the September 11th attack, the carrier's commander was able to draw on networked information provided by a variety of sensors to confidently increase the number of aircraft that were redirected in flight to targets in Afghanistan.

We continue to give emphasis to those activities and programs that demonstrate our ability to improve battlefield performance, and which contribute to the underlying suite of capabilities needed to ensure reliable, dynamic information.

DENY ENEMY ADVANTAGES AND EXPLOIT WEAKNESSES

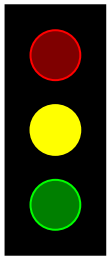
Our national security depends on clear, unambiguous, comprehensive, actionable intelligence – and aggressive counter-intelligence is vital to successful military planning and operations. Effective counter-intelligence can offer military planners "more preventative, less punitive" options that will neutralize or influence an adversary, but are short of using combat force.

In April 2002, we established a Defense Counterintelligence Field Activity to oversee all defense counterintelligence efforts, providing a "common operational counterintelligence picture" to monitor defense-wide threats and activities that could pose harm to our people or institutions. The Joint Counter-Intelligence Training Academy and the Defense Polygraph Institute are examining new methods for conducting counterintelligence and training counterintelligence officers to make counterintelligence part of integrated campaign planning and execution. The Under Secretary of Defense for Intelligence, established in FY 2003, is leading the intelligence community in developing a strategy that looks at long-term outcomes, exploring ways to integrate counterintelligence into campaign planning and execution.

By the end of FY 2005, our goal is to fill 95 percent of counter-intelligence billets at Joint Terrorism Task Force offices in the United States, and fully fund and staff 100 percent of the Force Protection Detachments approved by the Department of State. We will establish counter-intelligence elements at U.S. Northern Command,

which has responsibility for homeland defense, and resolve or otherwise dispose of 90 percent of all open terrorism investigations. Finally, we will sponsor three major advanced technology demonstrations during FY 2004, and one event in FY 2005.

DEFINE SKILLS AND COMPETENCIES FOR THE FUTURE



"A key roadblock to progress is a lack of understanding of key aspects of human and organizational behaviors…"

DoD Report to Congress on Network Centric Warfare
July 2001

Strategic Transformation Appraisal

History has shown that rapid and unexpected change can transform the geopolitical landscape. New technologies can revolutionize the character of armed conflict in ways that render previous doctrine and capabilities obsolete. Although contending with such uncertainty is a key challenge for the Department, certain features and trends of the security environment not only define today's geopolitical and military-technical challenges, but also highlight critical challenges that we must master in the future.

One trend is clear: the Department's transformation will be shaped by the emerging realities of the information age. Just as the move from the industrial age to the information age is changing the relative value of the sources of economic wealth (land, capital and labor), it is also altering the relative value of capabilities, assets, and skills that underwrite national security. Processes and organizations that cannot adapt to a networked, interoperable environment will not provide the knowledge, speed, precision, and agility we will need in the future.

More important, old ways and thinking will not foster the *human* skills demanded by our emerging security environment. Intellectual agility, adaptability, and the capacity to act in the midst of dynamic

complexity and uncertainty have increased importance in information-age warfare.

Today we are taking the first steps toward evolving our training and education to build the future force: we are establishing information-age warfare chairs at defense educational institutions; funded cutting edge research by defense educational institutions and their research partners, and founded a Transformation Certificate program for the National Security Executive Education Program sponsored by the National Defense University.

To guide transformation efforts across the Department, the Secretary issued his Transformation Planning Guidance in April 2003. This documents lists defense-wide priorities for fostering and promoting innovation. Subsequently, the military services and the U.S. Joint Forces Command prepared individual "transformation roadmaps" to describe how they are using concept-based experimentation, educational and training programs, operational prototypes, and other approaches to drive change. The first of these annual roadmaps were submitted in the fourth quarter of FY 2002, and updated during the first quarter of FY 2004. They complement the resource planning process, define a shared future vision, and provide actionable language for implementation. They become the baseline for managing transformational change and risk. The Transformation Planning Guidance and service roadmaps can be viewed at www.oft.osd.mil.

Are we making progress toward our transformational goals? To help keep the Department on track, the Director of the Office of Force Transformation prepares an annual assessment of progress being made toward transformational goals. The first of these Strategic Transformation Appraisals was completed in January 2004. Beginning in FY 2005, this classified report will be submitted each November to the Secretary of Defense. The appraisal will emphasize defense-wide transformational trends and recommend whether plans or resources should be adjusted to maintain progress toward the Secretary's transformational priorities.

The January 2004 appraisal indicated where information-age trends are taking the Department, and pointed to where we must go to strengthen the training and education:

2003	2004
• More expeditionary • More networked • Designed to leverage the exterior positions • Leverage increasingly persistent intelligence, surveillance, and reconnaissance • Tighter sensor-shooter timelines • Value information superiority • Joint interoperability at the operational level • Focus on unmanned capabilities	• Lighter, more agile, easily deployable units • Knowledge-enabled warfare • Improve vertical / horizontal intelligence distribution • Strengthen intelligence capabilities for the 21st century • Joint force synergy • Demand-centered intelligence • Jointness to the lowest appropriate level • Substitution of capital for labor

Optimize Intelligence Capabilities

ESTABLISH DEFENSE INTELLIGENCE AND SECURITY STRATEGY, POLICY, AND RELATED PROCESSES

During FY 2003, we established an Under Secretary of Defense for Intelligence to ensure military intelligence capabilities respond to the needs of both the Secretary of Defense and the Director of Central Intelligence. Drawing on a best practice from private industry, Defense and Director of Central Intelligence planners are working to synchronize their individual strategies and to reconcile their performance planning and measurement requirements. This will lead to a single performance measurement cycle for defense intelligence components, and help streamline intelligence oversight functions.

DELIVER A RESTRUCTURED AND PROACTIVE DEFENSE HUMAN INTELLIGENCE CAPABILITY, SATISFYING COMBATANT COMMANDERS' FULL SPECTRUM OF REQUIREMENTS AND SUPPORTING THE NEEDS OF POLICY-MAKERS

A re-invigorated human intelligence (HUMINT) capability is one of the leading indicators of transformation in the intelligence

community. HUMINT can provide keystone tactical and operational information to combatant commanders as part of integrated intelligence operations, and is a fundamental tool in the deterrence of adversaries. The challenge for the intelligence community brought by the global war on terror is to provide insights into goals, motivations, history, networks, relationships—all dimensions of human behavior—to a level of detail that is far greater than we can accomplish today. HUMINT is crucial to meeting this challenge.

During the first quarter of FY 2004, we outlined HUMINT reform proposals, identified which are the most critical to achieving our strategic goals, and recommended courses of action for FY 2005 and beyond to the Secretary and Congress.

DELIVER A HORIZONTALLY INTEGRATED NATIONAL SECURITY ENTERPRISE ENCOMPASSING JOINT, INTERAGENCY, AND MULTINATIONAL DATA, PROCESSES, AND CAPABILITIES IN COLLABORATION WITH THE DIRECTOR OF CENTRAL INTELLIGENCE

Another leading indicator of performance is Horizontal Integration: an entirely new perspective on how we collect, process, and apply intelligence. Horizontal integration focuses on outcomes – on what data is most usable to the most consumers, how easy it is to post and process across a network, and how seamlessly intelligence can be integrated into other defense activities.

Toward this goal, we have established a senior steering group with the Central Intelligence Agency to review current programs and processes, recommend changes, and propose measures of performance to be monitored over the long-term. Accordingly, we have also developed a phased investment plan that includes war-gaming, experiments, and demonstration projects.

ATTRACT, RECRUIT, RETAIN, AND REWARD HIGH QUALITY PEOPLE FROM GOVERNMENT, INDUSTRY, AND ACADEMIA

Perhaps the most important indicator of ability to meet our long-term strategic goals for intelligence is the quality of our intelligence analysts. We need energetic, dedicated people with broad and varied experiences. They must be problem-solvers who can operate effectively in an environment that constantly changes to meet new challenges and threats.

During FY 2005, and in concert with the National Security Personnel System (see Institutional Risk), we will stand up a Defense Civilian Intelligence Personnel System. The new system will tie performance to the defense intelligence strategy, and strive to improve job satisfaction by providing clear direction and quantitative objectives against which an employee can measure his or her progress.